

## Security Bulletin

# Vulnerabilities in Intel SPP, TDX and VROC

Author(s) : Eviden PSIRT  
Reference : PSIRT-1732  
Created : 07 November 2024  
Version : 0.2  
Status : Neutralization  
TLP Classification : CLEAR  
Document date : 10 January 2025  
Keywords : CVE-2024-21850 CVE-2024-29079 CVE-2024-32485  
CVE-2024-36242 CVE-2024-38660

### **TLP:CLEAR**

*Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.*

**FOR PUBLIC USE**

## List of changes

Version	Date	Description
0.1	2024/11/14	Initial Eviden version
0.2	2025/01/10	TLP:CLEAR

## Executive summary

Potential security vulnerabilities in some Intel TDX Seamldr module software, Intel® Virtual RAID on CPU (Intel VROC) and SPP may allow escalation of privilege and denial of service. Intel is releasing software updates to mitigate this potential vulnerabilities.

Intel has indicated that those two vulnerabilities CVE-2024-36242, CVE-2024-38660 directly relate to the Sapphire Rapids and Emerald Rapids.

All vulnerabilities result from incorrect settings of the VMM Hypervisor. No firmware BIOS update should be expected to fix them.

## Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
<a href="#">CVE-2024-21850</a>	6.0	AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N
<a href="#">CVE-2024-29079</a>	6.8	AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L
<a href="#">CVE-2024-32485</a>	3.9	AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L
<a href="#">CVE-2024-36242</a>	8.8	AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
<a href="#">CVE-2024-38660</a>	3.8	AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Eviden is liaising closely with its suppliers and investigating the exact nature of these vulnerabilities to provide validated remediation.

## Affected products

Products	Fixed version	Status	Comments
TDX Seamldr	1.5.02.00	Fixed	
VROC	8.6.0.3001	Fixed	
SPP	N/A		

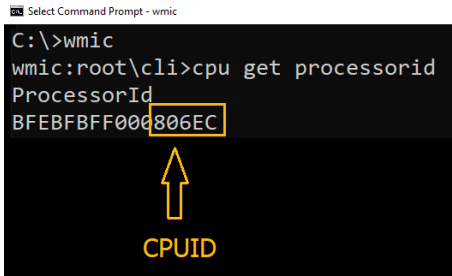
The products are affected according to the precise versions of processor embedded. The Intel processors report their precise version through the CPUID instruction.

## Windows operating systems

Follow [Intel's instruction](#) to get your CPUID. The CPUID is part of the processor ID.

```

Select Command Prompt - wmic
C:\>wmic
wmic:root\cli>cpu get processorid
ProcessorId
BFEBFBFF000806EC
    
```



## Linux operating systems

To obtain the CPUID of your Intel CPU, use the following command.

```

lscpu | awk '\
($1 == "Model:") {m1=$2/16; m2=$2%16}\
($1 == "Stepping:") {step=$2}\
($1 " " $2 == "CPU family:") {family=$3}\
END {printf("%.1x%.2x%.1x%.1x\n", m1, family, m2, step)} '
    
```

```

$ lscpu | awk '\
($1 == "Model:") {m1=$2/16; m2=$2%16}\
($1 == "Stepping:") {step=$2}\
($1 " " $2 == "CPU family:") {family=$3}\
END {printf("%.1x%.2x%.1x%.1x\n", m1, family, m2, step)} '
806ec
$
    
```

## List of affected CPUID

The reference for affected CPUID is Intel's [consolidated list of affected processors](#). The affected CPUID that you may find in BullSequana platforms are of the following type:

Component name	CPUID	MCU	Comments
Sapphire Rapids	806F7	2b000590	fixing is part of update software
Sapphire Rapids	806F8	2c000360	fixing is part of update software
Emerald Rapids	C06F2	0x21000200	fixing is part of update software

## List of Enterprise and Edge servers

The table below provides the Technical State to apply to implement Intel mitigation measures.

CVE	CVSS Score	Atos QLM	Bull Sequana S	Bull Sequana M	Bull Sequana x800	Bull Sequana SH	Bull Sequana SA11i, SA21i, SA21Si
<b>Recommended</b>							
<a href="#">CVE-2024-36242</a>	8.8	Unpatched	Unpatched	Unpatched	Unpatched	Unpatched	Unpatched
<a href="#">CVE-2024-38660</a>	3.8	Unpatched	Unpatched	Unpatched	Unpatched	Unpatched	Unpatched

### List of HPC products

The table below provides the Technical State to apply to implement Intel mitigation measures.

CVE	CVSS Score	Bull Sequana X400	Bull Sequana 400-E7	Bull Sequana XH2140 (C4E)	Bull Sequana XH3140
<b>Recommended</b>		<b>TBD</b>	<b>TBD</b>	<b>TBD</b>	<b>TBD</b>
<a href="#">CVE-2024-36242</a>	8.8	Unpatched	Unpatched	Unpatched	Unpatched
<a href="#">CVE-2024-38660</a>	3.8	Unpatched	Unpatched	Unpatched	Unpatched

### Recommendations

Eviden recommends applying its Technical States upgrade on its servers as soon as they are made available.

For **VROC** Intel recommends updating Intel® VROC software to version 8.6.0.3001 or later.

For **TDX** Intel recommends updating to SEAMLDR version 1.5.02.00, available in Unified Post Launch Release 1 (UPLR1).

For **SPP** Intel is not aware of any mainstream VMM software that enables SPP. There is no action required in non-virtualized environments or where SPP is not used. In virtualized environment, Intel recommends the Virtual Machine Monitor (VMM, hypervisor) software should not enable the SPP feature by ensuring bit 23 is 0: "Sub-page write permissions for EPT" in secondary Processor-Based VM-

Execution Controls. This bit should be clear in the virtual machine control structure (VMCS) for each guest

## Available Vendor Patches

No validated patch is available at the time. Eviden is working with its suppliers to distribute updates as soon as possible.

Technical States links for Eviden servers are reminded in the table below.

Product	Technical State link
Bull Sequana S	<a href="https://support.bull.com/ols/product/platforms/bullion/bullsequana-s/dl/pkgf/technical-state-dvd-packages">https://support.bull.com/ols/product/platforms/bullion/bullsequana-s/dl/pkgf/technical-state-dvd-packages</a>
Bull Sequana SA	<a href="https://support.bull.com/ols/product/platforms/bullion/bullsequana-sa-servers/dl/pkgf/pkg">https://support.bull.com/ols/product/platforms/bullion/bullsequana-sa-servers/dl/pkgf/pkg</a>
Bull Sequana SH	<a href="https://support.bull.com/ols/product/platforms/bullion/bullsequana-sh/dl/pkgf/pkg">https://support.bull.com/ols/product/platforms/bullion/bullsequana-sh/dl/pkgf/pkg</a>
Bull Sequana E	<a href="https://support.bull.com/ols/product/platforms/bullion/bullsequana-edge-servers/dl/pkgf/pkgf">https://support.bull.com/ols/product/platforms/bullion/bullsequana-edge-servers/dl/pkgf/pkgf</a>
Bull Sequana X1000	<a href="https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x1000/dl/pkgf/pkg">https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x1000/dl/pkgf/pkg</a>
Bull Sequana XH2000	<a href="https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/xh2000/dl/pkgf/pkg">https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/xh2000/dl/pkgf/pkg</a>
Bull Sequana XH3000	<a href="https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/xh3000/dl/pkgf/pkg">https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/xh3000/dl/pkgf/pkg</a>
Bull Sequana X400-E5	<a href="https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkgx400e5">https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkgx400e5</a>
Bull Sequana X400-E7	<a href="https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkgx400e7">https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkgx400e7</a>
Bull Sequana X400-A5	<a href="https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkgx400a5">https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkgx400a5</a>
Bull Sequana X400-A6	<a href="https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkgx400a6">https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x400/dl/pkgf/pkgx400a6</a>
Bull Sequana X550	<a href="https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x550">https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x550</a>
Bull Sequana X800 / QLM	<a href="https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x800/dl/pkgf/pkg">https://support.bull.com/ols/product/platforms/hw-extremcomp/sequana/x800/dl/pkgf/pkg</a>

## Available Workarounds

No workaround is available.

## Available Mitigations

No mitigation identified.

## Available Exploits/PoC

Eviden is not aware of any exploitation of the reported vulnerabilities.

## References

- 1.

## Glossary of terms

Term	Description
Mitigation	Refers to a setting, common configuration, or general best-practice, existing in a default state that could reduce the severity of exploitation of a vulnerability
Neutralization	The neutralization phase is the decision-making process during which the risk posed by an incident is evaluated.
PoC	Proof of Concept
Remediation	The remediation phase ends with the delivering of a qualified solution/update fixing the vulnerability without regression.
TI	Threat Intelligence
TLP	Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0. <a href="https://www.first.org/tlp/">https://www.first.org/tlp/</a>
Workaround	Refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update

## About this document

Eviden continuously monitors the security of its products. This Security Bulletin is shared under the constraints of the FIRST Traffic Light Protocol version 2.0 (TLP) to bring the attention of owners of the potentially affected Eviden products. Eviden recommends that all product owners determine whether the described situation is applicable to their individual case and take appropriate action.

Although Eviden tries to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information is provided “as is” without warranty of any kind. To the extent permitted by the Law, neither Eviden nor its affiliates, subcontractors or suppliers will be liable for incidental damages, downtime cost, lost profits, damages relating to the procurement of substitute products or services, or damages for loss of data, or software restoration. Product and company names mentioned herein may be trademarks of their respective owners.

The information in this document is subject to change without notice. The version of this document will be incremented according to the changes:

- Neutralization security bulletins are numbered 0.x
- Privately disclosed Remediation security bulletins are numbered 1.x
- Publicly disclosed Remediation security bulletins are numbered 2.x

Updated versions of this document can be found on:

- <https://support.bull.com/ols/product/security/psirt>

## About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The [purpose of Atos](#) is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

## About Eviden<sup>1</sup>

[Eviden](#) is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 53,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

---

<sup>1</sup> Eviden business is operated through the following brands: AppCentrica, ATHEA, BullSequana, Cloudamize, Cloudreach, Cryptovision, DataSentic, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, IDnomic, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Trustway, Visual BI, Worldgrid, X-Perion.

Eviden is a registered trademark. © Eviden SAS, 2025.